NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Visualization and Controls Program Peer Review 2006 AGA 12 Cryptographic Security Analysis

Tim Draelos, Principal Investigator

Sandia National Laboratories

(505) 844-8698

tjdrael@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

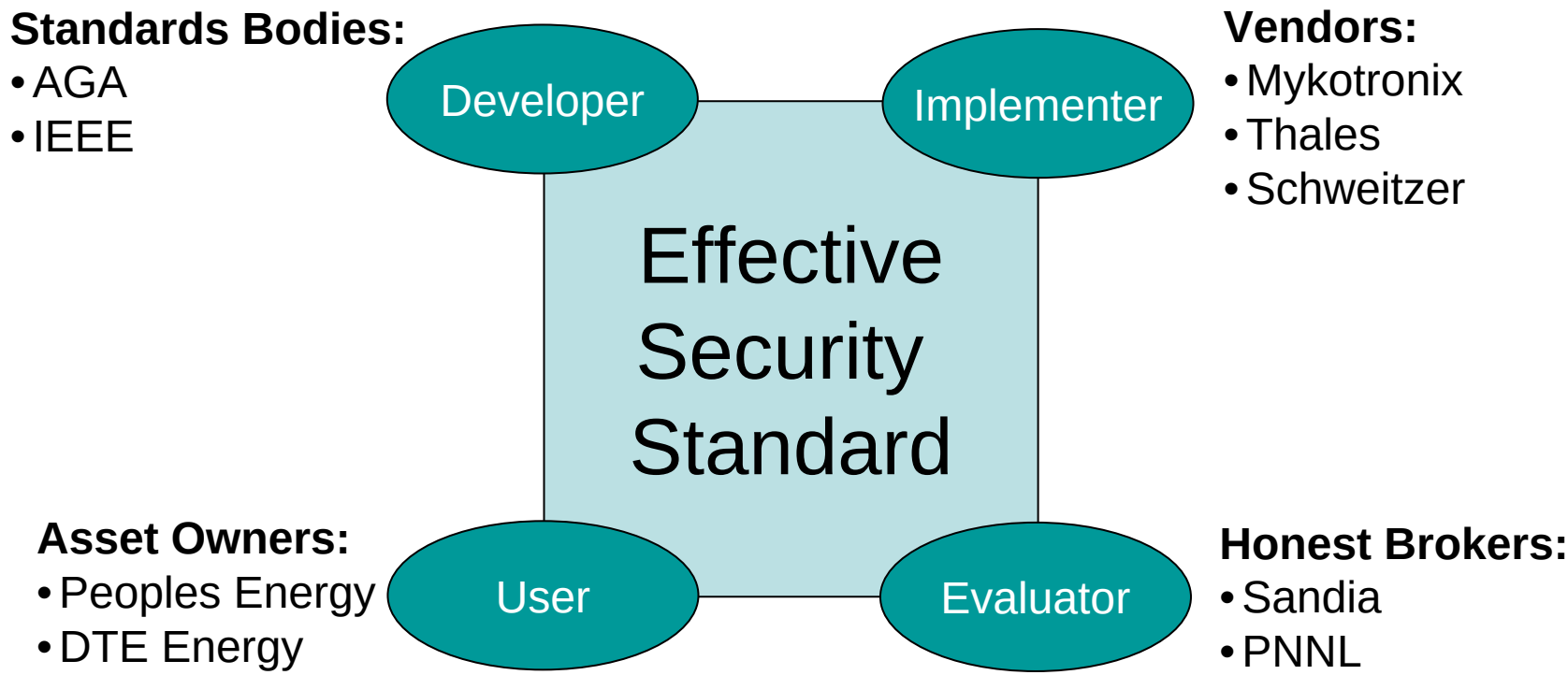
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Work Package Description

- NSTB FY05 Task
  - AGA 12: *Cryptographic Protection of SCADA Communications*
    - Part 1: Background, Policies, and Test Plan
    - Part 2: Retrofit Link Encryption for Asynchronous Serial Communications
    - Part 3: Protection of Networked Systems
    - Part 4: Protection Embedded in SCADA Components
  - Task 1: AGA 12, Part 2 Cryptographic Security Analysis
    - *AGA 12, Part 2 Cryptographic Security Analysis* report delivered June, 2006
  - Task 2: AGA 12, Part 2 Cryptographic Security Testing
    - *SCADA Cryptographic Security Test Plan: General Guidance* delivered June, 2006

Industry Needs

- Asset owners need SCADA security products they can trust
  - Trust can come from Honest Broker evaluation
- Vendors need a stable security standard for development



Industry Benefits (Impacts)

- Original draft reviewed
  - May 12, 2005
- Recommendations had limited impact on intermediate drafts
  - November 29, 2005
  - January 25, 2006
- Final recommendations had huge impact on most recent draft
  - March 31, 2006

Technical Approach

- Cryptographic Security Analysis and Testing
  - Studied multiple drafts of AGA 12, Part 2
  - Engaged AGA 12, Part 2 authors in technical discussions via email and telephone to increase our understanding.
  - Developed block diagrams / flow charts of AGA 12, Part 2 protocols
  - Studied cryptographic algorithms and their uses as specified by AGA 12, Part 2
  - Documented security findings and recommendations
  - Reported findings and recommendations to AGA 12, Part 2 authors
  - Prepared final report based on findings, recommendations, and changes to AGA 12, Part 2
  - Prepared general guidance for testing SCADA security devices

Collaborations and Partnerships

- GTI
  - Bill Rush: Lead contact / editor of AGA 12
  - John Kinast: AGA 12 author
  - Aakash Shah: AGA 12 software implementer / tester
- Cisco
  - Andrew Wright: Lead technical author of AGA 12
- AGA
  - Host body for AGA 12
- PNNL
  - Mark Hadley: AGA 12 device performance testing

Technical Progress – Accomplishments

- Created diagrams for Serial SCADA Protection Protocol
  - Session Layer, Transport Layer
  - OPN, ACK, CLS, ERR Messages
- Cryptographic Security Findings / Recommendations
  - Static Session – used to transfer Dynamic session keys
    - Use of stream ciphers for Static Sessions should be prohibited
    - The state variable (32-bit random number) is too short
    - 64-128 bits of state variable recommended
  - Attacks against PE Mode with No Holdback
    - Block swapping is possible without CRC detection
    - Repeated state variables defeats CRC check
  - Perform Full Holdback Authentication of dynamic session headers
  - Rewrite standard to promote consistent, secure implementations

Technical Progress – Accomplishments

- Final Reports
  - AGA 12 Part 2 Cryptographic Security Analysis
    - Official Use Only
  - SCADA Cryptographic Security Test Plan: General Guidance
- Impact
  - Greatly increased the security of AGA 12